付録B　実験の手順

相互接続性確認 基本試験

Pre-Shared 接続試験

【試験目的】
IKE 相互認証方式で、Pre-Shard を使用した際の接続性の確認を行う。
【手順】
※IKE ネゴシエーションは、IKE View にて Capture し保存する。

1） パラメータパターン１ 接続性確認

①A，B 2 台の異なる IPSec 装置に、以下のパラメータを設定。

(ア)	暗号アルゴリズム	：DES-CBC
(イ)	Hash アルゴリズム	：MD5
(ウ)	ペイロード	：ESP
(エ)	認証アルゴリズム	：HMAC-MD5
(オ)	Group Description	：Group1
(カ)	Shard Secret key	：任意 （文字数制限等を確認）
(キ)	その他のパラメータ	：Key Life Time や ID タイプ等のパラメータは任意

②A の暗号対象ネットワーク上のクライアントから、B の暗号対象ネットワーク上のクライアントに Ping を行い SA が確立され、IPSec 通信が正常に行える事を確認する。
③IPSec 機器の再起動等を行い、②で確立した SA を削除する。
④B の暗号対象ネットワーク上のクライアントから、A の暗号対象ネットワーク上のクライアントに Ping を行い S が確立され、IPSec 通信が正常に行える事を確認する。

2） パラメータパターン 2 接続性確認

① A，B 2 台の異なる IPSec 装置に、以下のパラメータを設定。

(ア)	暗号アルゴリズム	：DES-CBC
(イ)	Hash アルゴリズム	：SHA-1
(ウ)	ペイロード	：ESP
(エ)	認証アルゴリズム	：HMAC-SHA
(オ)	Group Description	：Group1
(カ)	Shard Secret key	：任意（文字数制限等確認）
(キ)	その他のパラメータ	：Key Life Time や ID タイプ等のパラメータは任意

② 上記（1）-②～④を繰返す。

【結果】

以下の試験結果マトリックスに試験結果を記入

1. Pre-Shared接続試験

試験実施日時：

製品 A　：
Version　：
Platform　：
担当　　：

製品 B　：
Version　：
Platform　：
担当　　：

1）パラメータパターン1 接続性確認

		Initiater				備考
		製品A		製品 B		
		結果	LOGファイル名	結果	LOGファイル名	
Responder	製品 A			○	1-1-B-A.log	
	製品 B	○	1-1-A-B.log			

2）パラメータパターン2 接続性確認

		Initiater				備考
		製品A		製品 B		
		結果	LOGファイル名	結果	LOGファイル名	
Responder	製品 A			○	1-2-B-A.log	
	製品 B	○	1-2-A-B.log			

記入方法
試験結果/ LOGファイル名 の形式で記入
試験結果は下記参照
正常にSA確立し、IPSec通信が行えた場合は ○を記入
SA確立に失敗し、IPSec通信が不能の場合　×を記入

ID ペイロードサポート確認

【試験目的】
各製品がサポートする Phase2 の ID ペイロードタイプを確認し、異なる ID ペイロードタイプを設定した時の接続性を確認する。
【手順】
※IKE ネゴシエーションは、IKE View にて Capture し保存する。
1）Phase2 ID ペイロードタイプの確認
①各製品がサポートする ID ペイロードタイプを確認し、下記のマトリックスに記入する。

2）異なる ID ペイロードタイプ使用時の接続性確認
一般的に使用される「ID_IPV4_ADDR」と「ID_IPV4_ADDR_SUBNET」の２つを例にし手順を示す。
①製品 A の ID ペイロードタイプに 「ID_IPV4_ADDR」を設定。製品 B の ID ペイロードタイプに「ID_IPV4_ADDR_SUBNET」を設定する。
（相互認証は Pre-Shard を使用し、その他のパラメータは任意の値を使用する。）
②A の暗号対象ネットワーク上のクライアントから、B の暗号対象ネットワーク上のクライアントに Ping を行い SA が確立され、IPSec 通信が正常に行える事を確認し、その際にどちらのパラメータが有効になっているかを確認する。
③IPSec 機器の再起動等を行い、②で確立した SA を削除する。
④B の暗号対象ネットワーク上のクライアントから、B の暗号対象ネットワーク上のクライアントに Ping を行い SA が確立され、IPSec 通信が正常に行える事を確認し、その際にどちらのパラメータが有効になっているかを確認する。
⑤製品 B の ID ペイロードタイプに「ID_IPV4_ADDR_SUBNET」を設定。製品 B の ID ペイロードタイプに「ID_IPV4_ADDR」を設定する。

⑥ ②～⑤を繰返す。

【結果】

以下の試験結果マトリックスに試験結果を記入

1. Phase2 IDサポート確認試験

1）Phase2 IDペイロードタイプの確認

試験実施日時：

製品名 ：
Version ：
Platform ：
担当 ：

IDペイロードタイプ	サポート	備考
IPV4_ADDR	○	
IPV4_ADDR_SUBNET	○	
IPV4_ADDR_RANGE		

記入方法
サポートするIDペイロードタイプに ○ を記入
上記以外をサポートする場合は、IDペイロードタイプ欄にサポートするタイプを記入する。

2)異なるIDペイロードタイプ使用時の接続性確認

試験実施日時：

製品 A ：
Version ：
Platform ：
担当 ：

製品 B ：
Version ：
Platform ：
担当 ：

			Initiater							
			製品A				製品B			
			IPV4_ADDR		IPV4 Subnet		IPV4_ADDR		IPV4 Subnet	
			結果	LOGファイル名	結果	LOGファイル名	結果	LOGファイル名	結果	LOGファイル名
Responder	製品A	IPV4_ADDR							○	2-2-B-A.log
		IPV4_Subnet								
	製品B	IPV4_ADDR	○	2-2-A-B.log						
		IPV4_Subnet								

記入方法
試験結果/ LOGファイル名 の形式で記入
試験結果は下記参照
正常にSA確立し、IPSec通信が行えた場合は、
SA確立に失敗し、IPSec通信が不能の場合

○を記入
×を記入

通信中リキー動作確認

【試験目的】

各製品がサポートする SA Life Type(SA 有効種類)を確認し、通信中に SA Duration（SA 有効期間）を迎えた際に、正常に Re-key が行われ通信が途絶えない事を確認する。

【手順】

1) SA Life Type の確認

①製品サポートする SA Life Type を確認する。

②それぞれの SA Life Type の設定値の最小値，最大値を確認する。

2) 通信中 Re-key 動作の確認

①製品 A の Life Duration を出来るだけ小さく設定。製品 B はそれよりも出来るだけ大きい値を設定。

②暗号対象ネットワーク上のクライアントから、Peer の暗号対象ネットワーク上のクライアントに Ping 等で通信を行い SA が確立され、IPSec 通信が正常に行える事を確認する。

③Ping 等で IPSec 通信を継続して行い通信中に Re-key を発生させ､通信が途絶えない事を確認

④ftp 等の tcp で IPSec 通信を継続して行い通信中に Re-key を発生させ、通信が途絶えない事を確認

⑤製品 B の Life Duration を出来るだけ小さく設定。製品 B は、それよりも出来るだけ大きい値を設定。

⑥ ②～⑤を繰返す。

【結果】

以下の試験結果マトリックスに試験結果を記入

3. 通信中Re-key動作確認試験

1）SA Life Type確認

製品名：VPN-1
Version：v4.1 sp2

SA Life Type	SA Duration				備考
	Phase1		Phase2		
	最小値	最大値	最小値	最大値	
Sec	10min	10080min	2min	1440min	

記入方法
SA Life Typeには、「Sec」または、「Byte」を記入
SA Durationの単位は、任意の単位を記入

運用性確認 基本試験

IP フラグメンテーション

【試験目的】
IPSEC 装置でフラグメンテーション発生時の IPsec 通信を確認する。IP フラグメンテーションが発生しても、IPsec 通信が可能であるかを確認する。
具体的には、平文では MTU 以下であるパケットが、ＥＳＰになったときに MTU を超える場合にフラグメントして通信可能であるか、以下２パターンで確認する。
　１）平文に Don't Fragment ビットがセットされていない場合
基本的なフラグメント処理を確認する
　２）平文に Don't Fragment ビットがセット場合されている場合
DF をセットした際のデータの取り扱い判断を確認する
DF セットしたときのフラグメンテーション動作はさらに PMTU のサポートが確認項目として挙げられる。ESP の経路に MTU が小さく設定された区間が存在した場合ゲートの外 (非安全) 側より内側に対してアナウンスがなされなければならない。今回設定された実験環境では PMTU についての試験は行うことができない。次回以降への課題項目である。

【仕様確認】
IPSEC 装置が RFC1191 PMTU（Path MTU Discovery）をサポートしているかをチックシートに記載する。
【手順】
1)DF フラグ OFF のとき
端末(Windows のコマンドラインで説明)のコマンドラインから ping コマンドでデータ長が 1440byte*パケットを送信する。

>ping –l 1440 [相手ゲートの端末]

*ESP 処理後に 1518byte となりフラグメンテーション処理が行なわれる
通信が失敗した場合はパケットログ、製品から出力記録されるログより原因を分析し理由とともにチェックシートに記入する。
対向機器の端末からも同様の実験を行う。

2)DF フラグ ON のとき
双方、または一方の機器が DF セット時に ESP 処理を行わない場合はこの試験を見送る。ただし、どちらか一方でも DF セット時の動作を確認していない場合はこの手順を実行する。
端末のコマンドラインから ping コマンドでデータ長が 1440byte、DF がセットされたパケットを送信する。

>ping –l 1440 –f [相手ゲートの端末]

通信が失敗し、メッセージがタイムアウトであった場合は ESP が送信されて返信が無いことを確認する。
通信が失敗し、メッセージが「Packet needs to be fragmented but DF set.」であった場合はゲートと端末の間のパケットを採取し ICMP(Destination Unreachable: fragmentation needed and DF set) が返されていることを確認する
対向機器の端末からも同様の実験を行う。

【結果】

DATE：

チェックシート記載ベンダー、ご担当者名
：
：
IPSEC装置A　装置名：
ベンダー名：
ご担当者名：
装置バージョン：

IPSEC装置B　装置名：
ベンダー名：
ご担当者名：
装置バージョン：

仕様確認）

IPSEC装置A　装置名：	IPSEC装置B　装置名：
・RFC1191サポート　○orNG　＿＿＿＿	・RFC1191サポート　○orNG　＿＿＿＿
・他の仕様の場合　サポート仕様、方法を記載	・他の仕様の場合　サポート仕様、方法を記載

1）平文にDon't Fragmentビットがセットされていない場合

・IPSEC装置A→B　ping -t -l 1440 ping応答　○orNG ・NGの場合の状況、データ等を記録	・IPSEC装置B→A　ping -t -l 1440 ping応答　○orNG ・NGの場合の状況、データ等を記録

2）平文にDon't Fragmentビットがセットされている場合

・IPSEC装置A→B　ping -t -l 1440 -f PMTU送出確認○orNG IKEVIEWファイル名 ping応答　○orNG ・NGの場合の状況、データ等を記録	・IPSEC装置B→A　ping -t -l 1440 -f PMTU送出確認○orNG IKEVIEWファイル名 ping応答　○orNG ・NGの場合の状況、データ等を記録

SA 消失試験

【目的】

IPsec 機器が故障あるいは停電などの理由で SA を消失した後に復旧する際の各製品の挙動、および復旧手順を確認する

まず、各々の SA を消去する機能を調査する。

前項の調査に基づき実際に機器を再起動やなどを行ながら通信回復の試験を行う。

【手順】

SA 削除の機能確認

Phase2 の SA のみを消去できるか､特定のセッションの SA を消去できるかを調査する

Phase1 の SA を消去できるか､特定の機器との SA を消去できるかを調査する

SA 消失後の復旧手順確認

次の 3 段階の組み合わせで行う。それぞれの指示は組み合わせリストに従う。

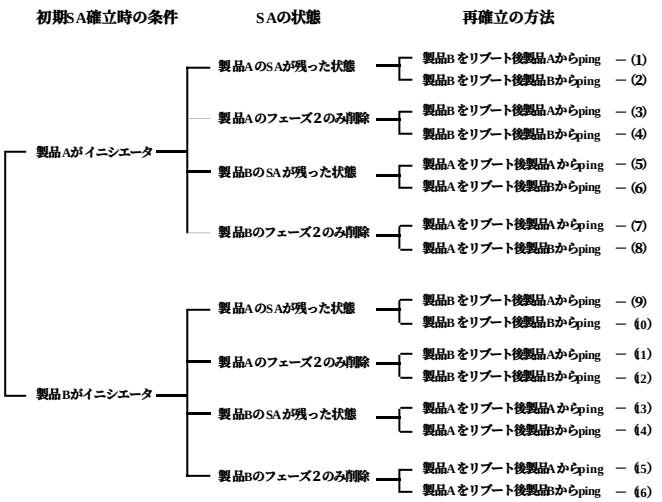
① 初期 SA 確立時の条件
イニシエータに指定された機器から SA を作成させる。

② SA 状態(操作)
指定された機器の SA 情報をそのまま､またはフェーズ 2 SA を削除する。

③ 再確立の方法 1 -片側機器の再起動-
指定された機器を再起動する

④ 再確立の方法 2 -ping コマンドによる SA 回復の試行-
指定された機器の配下に在る PC から ping コマンドでゲート間のトラフィックを発生させて反応を観察する。

組み合わせ表



【結果】

SA消失に関する試験の手順　(フォーム2)

＜SA再構築試験＞

記録日	2001年1月24日
製品Aの名称	
ベンダー名	
製品Bの名称	
ベンダー名	
記録者名	

初期SA確立時の条件	SAの状態	リブートした側	pingした側	結果	備考
Aがイニシエーター	AのSAが残った状態	Bをリブート	Aからping		
		Bをリブート	Bからping		
	Aのフェーズ２のみ削除	Bをリブート	Aからping		
		Bをリブート	Bからping		
	BのSAが残った状態	Aをリブート	Aからping		
		Aをリブート	Bからping		
	Bのフェーズ２のみ削除	Aをリブート	Aからping		
		Aをリブート	Bからping		
Bがイニシエーター	AのSAが残った状態	Bをリブート	Aからping		
		Bをリブート	Bからping		
	Aのフェーズ２のみ削除	Bをリブート	Aからping		
		Bをリブート	Bからping		
	BのSAが残った状態	Aをリブート	Aからping		
		Aをリブート	Bからping		
	Bのフェーズ２のみ削除	Aをリブート	Aからping		
		Aをリブート	Bからping		

※　「結果」には条件に相当する以下の記号を入れてください。
　◎：　おおよそ10秒でSAの再構築ができた。　○：　10～60秒 かかってSAの再構築ができた。
　△：　再確立まで60秒以上かかった。　×：　再確立できない。　－：　試験せず。(フェーズ２のみ消せないなどの理由で)
※◎以外は「備考」欄に簡単に状況を記述ください。「何秒でつながった」「繰り返しエラーを発し結局再確立できなかった」など
※気がついたことがあれば◎の場合でもコメントを記述ください。「エラーを何回発したら自動的にリブートして再確立した」「再確立した際、古いSAが
残った。SA Life Time後古いSAは消えた」など

END to END 通信確認

【目的】

試験手順を作成するにあたり試験の内容を考察する

○TCP 通信試験

TCP/IP は経路上におけるデータの保護を行うためにセッションを維持している。また TCP のセッションを用いるアプリケーション(Telnet, FTP など)で取り扱われるデータは送信元と受信先で同じデータでにならなければならない。このため接続実験では FTP によるファイル転送を採用し、通信開始と完了を確認する。

○UDP 通信試験

UDP は TCP に比較してセッションを維持せずに通信を行う。使用するアプリケーションは LAN であることを前提条件にした TFTP など、データの完全な一致を必要としないストリーミング系などがある。今回の試験では TFTP をアプリケーションとして採用するが、将来的には電子会議室システムなど実際に使用される可能性の高いアプリケーションでテストを行うことが望ましいと考える。

【手順】

環境の確認

以下のアプリケーションをクライアント側サブネットのシステムに用意する。

FTP サーバ、FTP クライアント TFTP サーバ、TFTP クライアント

実験前の確認項目

IKEview は外側のセグメントに配置して IKE を収集する。ftp によるファイル転送中に re-key が行われることを確認する(re-key は可能な条件すべて行う。行われた場合はその可否と Ph2 か Ph1，2 両方であることを明記する)。

実験手順

TCP: ftp

1. 製品 A の配下の PC (A) より製品 B の配下の PC(B) に対して ftp セッションを開始する。PC(B)のファイルを get コマンドで取り込む
2. 転送が終わったファイルのファイルサイズを確認して転送もとのファイルと同じことを確認する。IKEview のログで re-key が行われることを確認する。
3. A、B の関係を入れ替えて１，２の手順を繰り返す。

UDP: tftp

1. 製品 A の配下の PC (A) より製品 B の配下の PC (B) に対して tftp セッションを開始する。PC(B)のファイルを put コマンドで取り込む
2. 転送が終了することを確認する。
3. A，B の関係を入れ替えて１，２の手順を繰り返す。

【結果】

6.END to END通信試験

製品A　　機器名＿＿＿＿＿＿＿＿
プラットフォーム＿＿＿＿＿＿＿＿
バージョン［/プラットフォーム］＿＿＿＿＿＿＿＿
担当者名＿＿＿＿＿＿＿＿

製品B　　機器名＿＿＿＿＿＿＿＿
プラットフォーム＿＿＿＿＿＿＿＿
バージョン［/プラットフォーム］＿＿＿＿＿＿＿＿
担当者名＿＿＿＿＿＿＿＿

initiator&Client	TCP[ftp]	UDP[tftp]	備考
A			
B			

注)イニシエータはアプリケーションのクライアント側であること。レスポンダになる場合はそのことを明記する。
FTPによるファイル転送はファイルサイズを比較して一致した場合に○をつける。それ以外は×。
TFTPによるファイル転送は完了することのみを条件として○をつける。